

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

Applicants: Kazuhiko TAKABAYASHI et al.

International Application No.: PCT/JP2004/003336

International Filing Date: March 12, 2004

For: DEVICE-TO-DEVICE AUTHENTICATION SYSTEM,
DEVICE-TO-DEVICE AUTHENTICATION METHOD,
COMMUNICATION APPARATUS, AND COMPUTER
PROGRAM

745 Fifth Avenue
New York, NY 10151

EXPRESS MAIL

Mailing Label Number: EV206809967US

Date of Deposit: January 11, 2005

I hereby certify that this paper or fee is being deposited with the United States Postal Service "Express Mail Post Office to Addressee" Service under 37 CFR 1.10 on the date indicated above and is addressed to Mail Stop PCT, Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.

Adam Ahmed
(Typed or printed name of person mailing paper or fee)

A. Ahmed
(Signature of person mailing paper or fee)

CLAIM OF PRIORITY UNDER 37 C.F.R. § 1.78(a)(2)

Mail Stop PCT
Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

Sir:

Pursuant to 35 U.S.C. 119, this application is entitled to a claim of priority to Japan
Application No. 2003-132903 filed 12 May 2003.

Respectfully submitted,

FROMMER LAWRENCE & HAUG LLP
Attorneys for Applicants

By: William S. Frommer
William S. Frommer
Reg. No. 25,506
Tel. (212) 588-0800

10/520975

Rec'd PTO 11 JAN 2005
PCT/JP 2004/003336日 本 国 特 許 庁
JAPAN PATENT OFFICE

12.3.2004

別紙添付の書類に記載されている事項は下記の出願書類に記載されている事項と同一であることを証明する。

This is to certify that the annexed is a true copy of the following application as filed with this Office.

出 願 年 月 日 2 0 0 3 年 5 月 1 2 日
Date of Application:

出 願 番 号 特 願 2 0 0 3 - 1 3 2 9 0 3
Application Number:
[ST. 10/C] : [J P 2 0 0 3 - 1 3 2 9 0 3]

出 願 人 ソニー株式会社
Applicant(s):

REC'D 29 APR 2004

WIPO

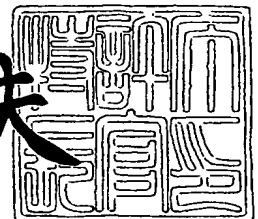
PCT

PRIORITY DOCUMENT
SUBMITTED OR TRANSMITTED IN
COMPLIANCE WITH
RULE 17.1(a) OR (b)

2 0 0 4 年 4 月 1 6 日

特許庁長官
Commissioner,
Japan Patent Office

今 井 康 夫



出証番号 出証特 2 0 0 4 - 3 0 3 2 1 3 1

【書類名】 特許願

【整理番号】 0390411004

【提出日】 平成15年 5月12日

【あて先】 特許庁長官殿

【国際特許分類】 G06F 17/60

【発明者】

【住所又は居所】 東京都品川区北品川 6 丁目 7 番 3 5 号 ソニー株式会社
内

【氏名】 高林 和彦

【発明者】

【住所又は居所】 東京都品川区北品川 6 丁目 7 番 3 5 号 ソニー株式会社
内

【氏名】 中野 雄彦

【発明者】

【住所又は居所】 東京都品川区北品川 6 丁目 7 番 3 5 号 ソニー株式会社
内

【氏名】 本田 康晃

【発明者】

【住所又は居所】 東京都品川区北品川 6 丁目 7 番 3 5 号 ソニー株式会社
内

【氏名】 五十嵐 卓也

【特許出願人】

【識別番号】 000002185

【氏名又は名称】 ソニー株式会社

【代理人】

【識別番号】 100093241

【弁理士】

【氏名又は名称】 宮田 正昭

【選任した代理人】

【識別番号】 100101801

【弁理士】

【氏名又は名称】 山田 英治

【選任した代理人】

【識別番号】 100086531

【弁理士】

【氏名又は名称】 澤田 俊夫

【手数料の表示】

【予納台帳番号】 048747

【納付金額】 21,000円

【提出物件の目録】

【物件名】 明細書 1

【物件名】 図面 1

【物件名】 要約書 1

【包括委任状番号】 9904833

【プルーフの要否】 要

【書類名】 明細書

【発明の名称】 機器間認証システム及び機器間認証方法、通信装置、並びにコンピュータ・プログラム

【特許請求の範囲】

【請求項 1】

ルータ経由で外部ネットワークに接続可能なホーム・ネットワーク上の機器を認証する機器間認証システムであって、

前記ホーム・ネットワーク上の機器に対してアクセスする他の機器が前記ホーム・ネットワーク上に存在するかどうかを確認するローカル環境管理手段を備える、

ことを特徴とする機器間認証システム。

【請求項 2】

一方の機器はコンテンツを正当に取得するホーム・サーバであり、他方の機器はホーム・サーバに対してコンテンツを要求し利用するクライアントであり、

双方の機器が同じホーム・ネットワーク上に存在することが確認されたことに応じて、前記ホーム・サーバは前記クライアントに対しコンテンツの提供及び／又はコンテンツに関するライセンスの発行を行なう、

ことを特徴とする請求項 1 に記載の機器間認証システム。

【請求項 3】

前記ホーム・ネットワーク上には 2 台以上のホーム・サーバを設置可能であり、

ホーム・サーバ毎に、同じホーム・ネットワーク上に存在することが確認されたクライアントに対しコンテンツの提供及び／又はコンテンツに関するライセンスの発行を行なう、

ことを特徴とする請求項 1 に記載の機器間認証システム。

【請求項 4】

クライアントは、同じホーム・ネットワーク上の 2 台以上のホーム・サーバからコンテンツの提供及び／又はコンテンツに関するライセンスの発行を受けることができる、

ことを特徴とする請求項 3 に記載の機器間認証システム。

【請求項 5】

クライアントは、同じホーム・ネットワーク上の複数のホーム・サーバから取得したコンテンツを利用可能であるが、別のホーム・ネットワーク上のホーム・サーバに接続した時点で、それ以外のホーム・ネットワーク上のホーム・サーバから取得したコンテンツを利用不能となる、

ことを特徴とする請求項 3 に記載の機器間認証システム。

【請求項 6】

前記ローカル環境管理手段は、アクセス要求元の機器の MAC アドレスが default Gateway に設定されているルータの MAC アドレスに一致しないかどうかによって同じホーム・ネットワーク上に存在するかどうかを確認する、

ことを特徴とする請求項 1 に記載の機器間認証システム。

【請求項 7】

前記ローカル環境管理手段は、各機器がホーム・ネットワークに関する同じ識別情報を共有するかどうかによって同じホーム・ネットワーク上に存在するかどうかを確認する、

ことを特徴とする請求項 1 に記載の機器間認証システム。

【請求項 8】

各機器は default Gateway に設定されているルータの MAC アドレスをホーム・ネットワークに関する識別情報として取得し、機器同士が同じ default Gateway の MAC アドレスを保持しているかどうかによって同じホーム・ネットワーク上に存在するかどうかを確認する、

ことを特徴とする請求項 7 に記載の機器間認証システム。

【請求項 9】

ホーム・ネットワーク上にネットワーク識別情報を供給するローカル環境管理装置を設置し、

各機器は前記ローカル環境管理装置の MAC アドレスをホーム・ネットワークに関する識別情報として取得し、機器同士が同じローカル環境管理装置の MAC

アドレスを保持しているかどうかによって同じホーム・ネットワーク上に存在するかどうかを確認する、
ことを特徴とする請求項 7 に記載の機器間認証システム。

【請求項 10】

ルータ経由で外部ネットワークに接続可能なホーム・ネットワーク上の機器を認証する機器間認証方法であって、

前記ホーム・ネットワーク上の機器に対してアクセスする他の機器が前記ホーム・ネットワーク上に存在するかどうかを確認するローカル環境管理ステップを備える、

ことを特徴とする機器間認証方法。

【請求項 11】

一方の機器はコンテンツを正当に取得するホーム・サーバであり、他方の機器はホーム・サーバに対してコンテンツを要求し利用するクライアントであり、

双方の機器が同じホーム・ネットワーク上に存在することが前記ローカル環境管理ステップにより確認されたことに応じて、前記ホーム・サーバは前記クライアントに対しコンテンツの提供及び／又はコンテンツに関するライセンスの発行を行なう、

ことを特徴とする請求項 10 に記載の機器間認証方法。

【請求項 12】

前記ホーム・ネットワーク上には 2 台以上のホーム・サーバを設置可能であり、

ホーム・サーバ毎に、同じホーム・ネットワーク上に存在することが確認されたクライアントに対しコンテンツの提供及び／又はコンテンツに関するライセンスの発行を行なう、

ことを特徴とする請求項 10 に記載の機器間認証方法。

【請求項 13】

クライアントは、同じホーム・ネットワーク上の 2 台以上のホーム・サーバからコンテンツの提供及び／又はコンテンツに関するライセンスの発行を受けることができる、

ことを特徴とする請求項 12 に記載の機器間認証方法。

【請求項 14】

クライアントは、同じホーム・ネットワーク上の複数のホーム・サーバから取得したコンテンツを利用可能であるが、別のホーム・ネットワーク上のホーム・サーバに接続した時点で、それ以外のホーム・ネットワーク上のホーム・サーバから取得したコンテンツを利用不能となる、

ことを特徴とする請求項 12 に記載の機器間認証方法。

【請求項 15】

前記ローカル環境管理ステップでは、アクセス要求元の機器の MAC アドレスが default Gateway に設定されているルータの MAC アドレスに一致しないかどうかによって同じホーム・ネットワーク上に存在するかどうかを確認する、

ことを特徴とする請求項 10 に記載の機器間認証方法。

【請求項 16】

前記ローカル環境管理ステップでは、各機器がホーム・ネットワークに関する同じ識別情報を共有するかどうかによって同じホーム・ネットワーク上に存在するかどうかを確認する、

ことを特徴とする請求項 10 に記載の機器間認証方法。

【請求項 17】

前記ローカル環境管理ステップにおいて、各機器は default Gateway に設定されているルータの MAC アドレスをホーム・ネットワークに関する識別情報として取得し、機器同士が同じ default Gateway の MAC アドレスを保持しているかどうかによって同じホーム・ネットワーク上に存在するかどうかを確認する、

ことを特徴とする請求項 16 に記載の機器間認証方法。

【請求項 18】

ホーム・ネットワーク上にネットワーク識別情報を供給するローカル環境管理装置が設置されており、

前記ローカル環境管理ステップにおいて、各機器は前記ローカル環境管理装置

のMACアドレスをホーム・ネットワークに関する識別情報として取得し、機器同士が同じローカル環境管理装置のMACアドレスを保持しているかどうかによって同じホーム・ネットワーク上に存在するかどうかを確認する、ことを特徴とする請求項16に記載の機器間認証方法。

【請求項19】

ルータ経由で外部ネットワークに接続可能なホーム・ネットワーク上で動作する通信機器であって、

自己が接続されているホーム・ネットワーク経由でアクセスする他の機器が同じホーム・ネットワーク上に存在するかどうかを確認するローカル環境管理手段を備える、ことを特徴とする通信機器。

【請求項20】

ホーム・ネットワーク上でコンテンツを提供するホーム・サーバとして動作し、

前記ローカル環境管理手段により同じホーム・ネットワーク上に存在することが確認された機器に対してのみコンテンツの提供及び／又はコンテンツに関するライセンスの発行を行なうコンテンツ提供手段をさらに備える、ことを特徴とする請求項19に記載の通信機器。

【請求項21】

ホーム・ネットワーク上でホーム・サーバに対してコンテンツを要求するクライアントとして動作し、

前記ローカル環境管理手段により同じホーム・ネットワーク上に存在することが確認されたホーム・サーバからのみコンテンツの提供及び／又はコンテンツに関するライセンスの発行を受けるコンテンツ利用手段をさらに備える、ことを特徴とする請求項19に記載の通信機器。

【請求項22】

前記ホーム・ネットワーク上には2台以上のホーム・サーバを設置可能であり、

前記コンテンツ利用手段は、前記ローカル環境管理手段により同じホーム・ネ

ットワーク上に存在することが確認された2台以上のホーム・サーバからコンテンツの提供及び／又はコンテンツに関するライセンスの発行を受けることができる、

ことを特徴とする請求項21に記載の通信機器。

【請求項23】

前記コンテンツ利用手段は、同じホーム・ネットワーク上の複数のホーム・サーバから取得したコンテンツを利用可能であるが、別のホーム・ネットワーク上のホーム・サーバに接続した時点で、それ以外のホーム・ネットワーク上のホーム・サーバから取得したコンテンツを利用不能となる、

ことを特徴とする請求項21に記載の通信機器。

【請求項24】

前記ローカル環境管理手段は、アクセス要求元の機器のMACアドレスがdefault Gatewayに設定されているルータのMACアドレスに一致しないかどうかによって同じホーム・ネットワーク上に存在するかどうかを確認する、

ことを特徴とする請求項19に記載の通信機器。

【請求項25】

前記ローカル環境管理手段は、各機器がホーム・ネットワークに関する同じ識別情報を共有するかどうかによって同じホーム・ネットワーク上に存在するかどうかを確認する、

ことを特徴とする請求項19に記載の通信機器。

【請求項26】

前記ローカル環境管理手段は、default Gatewayに設定されているルータのMACアドレスをホーム・ネットワークに関する識別情報として取得するとともに、通信相手が同じdefault GatewayのMACアドレスを保持しているかどうかによって同じホーム・ネットワーク上に存在するかどうかを確認する、

ことを特徴とする請求項25に記載の通信機器。

【請求項27】

ホーム・ネットワーク上にネットワーク識別情報を供給するローカル環境管理装置が設置されており、

前記ローカル環境管理手段は、前記ローカル環境管理装置のMACアドレスをホーム・ネットワークに関する識別情報として取得するとともに、通信相手が同じローカル環境管理装置のMACアドレスを保持しているかどうかによって同じホーム・ネットワーク上に存在するかどうかを確認する、
ことを特徴とする請求項25に記載の通信機器。

【請求項28】

ルータ経由で外部ネットワークに接続可能で、コンテンツを正当に取得するホーム・サーバとコンテンツを要求し利用するクライアントが存在するホーム・ネットワーク上において、機器を認証するための処理をコンピュータ・システム上で実行するようにコンピュータ可読形式で記述されたコンピュータ・プログラムであって、

前記ホーム・サーバと前記クライアントが前記ホーム・ネットワーク上に存在するかどうかを確認するローカル環境管理ステップと、

双方の機器が同じホーム・ネットワーク上に存在することが前記ローカル環境管理ステップにより確認されたことに応じて、前記ホーム・サーバは前記クライアントに対しコンテンツの提供及び／又はコンテンツに関するライセンスの発行を行なうコンテンツ提供ステップと、
を具備することを特徴とするコンピュータ・プログラム。

【発明の詳細な説明】

【0001】

【発明の属する技術分野】

本発明は、ネットワークなどによって配信される音楽データや画像データ、電子出版物などのデジタル・データや動画像などコンテンツの機器間での利用を管理する機器間認証システム及び機器間認証方法、通信装置、並びにコンピュータ・プログラムに係り、特に、著作権法で認められる私的使用の範囲内でコンテンツの利用を管理する機器間認証システム及び機器間認証方法、通信装置、並びにコンピュータ・プログラムに関する。

【0002】

さらに詳しくは、本発明は、ルータ経由で外部ネットワークに接続されているホーム・ネットワーク上で、著作権法で認められる私的使用の範囲内でコンテンツの利用を管理する機器間認証システム及び機器間認証方法、通信装置、並びにコンピュータ・プログラムに係り、特に、ホーム・ネットワーク上の各クライアント端末がホーム・サーバ上で正当に取得されているコンテンツを著作権法で認められる私的使用の範囲内で利用するように管理する機器間認証システム及び機器間認証方法、通信装置、並びにコンピュータ・プログラムに関する。

【0003】

【従来の技術】

近年のインターネットの普及により、コンピュータ・ファイルを始めとした各種のデジタル・コンテンツをネットワーク配信することが盛んに行なわれている。また、広帯域通信網（xDSL（x Digital Subscriber Line）、CATV（Cable TV）、無線ネットワークなど）の普及により、音楽データや画像データ、電子出版物などのデジタル・データや、さらには動画像などリッチ・コンテンツの配信もユーザにストレスなく伝送できるような仕組みが整いつつある。

【0004】

一方、配信されるコンテンツはデジタル・データであり、コピーや改竄などの不正な操作を比較的容易に行なうことができる。また、現在これらのコンテンツのコピーや改竄などの不正行為は頻繁に行なわれており、これがデジタル・コンテンツ・ベンダの利益を阻害する主要な要因となっている。この結果、コンテンツの値段も高くしなければならなくなり、普及の障壁となるという悪循環が起きている。

【0005】

例えば、最近では一般家庭内にもコンピュータやネットワークなどの技術が深く浸透してきている。家庭内のパーソナル・コンピュータやPDA（Personal Digital Assistants）などの情報機器、さらにはテレビ受像機やビデオ再生装置などの各種の情報家電がホーム・ネットワーク経由

で相互接続されている。また、このようなホーム・ネットワークは、多くの場合、ルータ経由でインターネットを始めとする外部の広域ネットワークに相互接続されている。そして、インターネット上のサーバから正当に取得されたコンテンツは、ホーム・ネットワーク上のサーバ（以下、「ホーム・サーバ」とも呼ぶ）に蓄積された後、家庭内の他の端末（クライアント）へホーム・ネットワーク経由で配信される。

【0006】

著作権法の下、著作物としてのコンテンツは無断の複製や改竄などの不正使用から保護を受ける。一方、著作物の正当な利用者においては、私的な使用、すなわち個人的に又は家庭内その他これに順ずる限られた範囲内において使用することを目的としてコンテンツを複製することが許されている（著作権法第30条を参照のこと）。

【0007】

この私的使用の範囲を上述したホーム・ネットワークにおいて適用した場合、ホーム・ネットワークに接続されているクライアント端末は、個人的又は家庭の範囲内での使用であると推定される。したがって、ホーム・サーバにおいて正当に取得されているコンテンツは、ホーム・ネットワーク上のクライアント端末は自由に使用することが相当であると思料される（勿論、コンテンツを享受できる端末の台数に一定の制限を設ける必要がある）。

【0008】

しかしながら、ホーム・ネットワーク上にログインしたクライアント端末が私的使用の範囲にあるかどうかを識別することは、現状の技術では困難である。

【0009】

例えば、ホーム・ネットワークはルータを介して外部のネットワークとIPプロトコル・ベースで相互接続されていることから、ホーム・サーバにとってはアクセスしてきたクライアントが実際にどこにいるのかは不明である。外部（遠隔）からのアクセスに対しホーム・サーバがコンテンツを提供してしまうと、コンテンツの利用はほぼ無制限となってしまう、コンテンツに関する著作権は保護されないに等しい。この結果、コンテンツ製作者は創作意欲を失いかねない。

【0010】

また、ホーム・サーバがホーム・ネットワーク内のクライアント端末に対して一様にコンテンツの利用を許可した場合、同じクライアント端末が時間差をおいて複数のホーム・ネットワークに跨ってログインすることにより、ほぼ無尽蔵にコンテンツを利用することが可能となってしまう。

【0011】

他方、クライアント端末に対して厳しい制限を課してしまうと、ユーザは、本来著作権法上で認められている私的使用を確保することができなくなってしまう。この結果、ユーザがコンテンツを十分に享受することができず、ホーム・サーバやコンテンツ配信サービスの利用が進まないために、コンテンツ事業の発展自体を阻害しかねない。

【0012】

例えば、著作物を正規に購入した利用者に自由利用が認められているということに鑑み、利用者がネットワーク上での情報を複製して利用するにあたって、コンテンツの権利保持者の理解が得られ易い方法に関する提案がなされている（例えば、特許文献1を参照のこと）。しかしながら、これは利用者を情報の利用権保持者との関係レベルによって分類し、関係レベル毎に異なる配信方法で情報を配信するというもので、ネットワーク上のどこまでが私的使用の範囲に該当するのかを識別するものではない。

【0013】

現在、ホーム・ネットワークを構成するプロトコルとして、例えばUPnP (Universal Plug and Play) が知られている。UPnPによれば、複雑な操作を伴うことなく容易にネットワークを構築することが可能であり、ネットワーク接続された機器間では困難な操作や設定を伴うことなくコンテンツ提供サービスを行なうことが可能となる。また、UPnPは、オペレーティング・システム(OS)に非依存であり、容易に機器の追加ができるという利点を持つ。

【0014】

UPnPでは、ネットワーク接続された機器間で、XML (eXtended

Markup Language) 形式で記述された定義ファイルを交換して相互認証を行なう。UPnPの処理の概要は以下の通りである。

【0015】

- (1) アドレッシング処理: IPアドレスなどの自己のデバイスIDを取得する
- (2) ディスカバリ処理: ネットワーク上の各デバイスの検索を行ない、各デバイスから受信した応答に含まれるデバイス種別や機能などの情報を取得する
- (3) サービス要求処理: ディスカバリ処理で取得された情報に基づいて各デバイスにサービスを要求する

【0016】

このような処理手順を行なうことで、ネットワーク接続された機器を適用したサービスの提供並びに受領が可能となる。新たにネットワークに接続される機器は、アドレッシング処理によりデバイスIDを取得し、ディスカバリ処理によりネットワーク接続されている他のデバイスの情報を取得し、サービス要求が可能となる。

【0017】

ホーム・サーバに格納されたコンテンツは、ホーム・ネットワーク上の他の機器からアクセス可能となる。例えば、UPnP接続を実行した機器によってコンテンツを取得することが可能である。コンテンツが映像データや音声データの場合、ネットワーク接続機器として、TVやプレーヤなどを接続すれば、映画や音楽を視聴することができる。

【0018】

しかし、ホーム・ネットワーク内の機器、例えばホーム・サーバには私的なコンテンツや有料コンテンツなど著作権管理を要求されるコンテンツが格納されていることから、不正アクセスの対策を考慮する必要がある。

【0019】

コンテンツの利用権(ライセンス)を有するユーザの機器によるアクセスは許容されて当然である。しかしながら、ホーム・ルータ経由で外部ネットワークに相互接続されているホーム・ネットワーク環境では、ライセンスを持たないユーザがホーム・ネットワークに入り込むことも可能である。

【0020】

不正アクセスを排除するため、例えば、ホーム・サーバにアクセスを許容するクライアントのリストを保持させ、クライアントからホーム・サーバへのアクセス要求が行なわれる度に、リストとの照合処理を実行して、不正アクセスを排除することができる。

【0021】

例えば、各通信機器に固有の物理アドレスであるMAC (Media Access Control) アドレスを用いてアクセス許容機器リストとして設定するMACアドレス・フィルタリングが知られている。すなわち、ホーム・ネットワークのような内部ネットワークと外部ネットワークとを隔離するルータ又はゲートウェイにアクセスを許容する各機器のMACアドレスを登録しておき、受信したパケットに付されているMACアドレスと登録されたMACアドレスとを照合し、未登録のMACアドレスを持つ機器からのアクセスを拒否する（例えば、特許文献2を参照のこと）。

【0022】

しかしながら、アクセス許容機器リストを構築するためには、内部ネットワークに接続されるすべての機器のMACアドレスを調べる必要があり、また、取得したすべてのMACアドレスを入力してリストを作成する手間が必要である。また、ホーム・ネットワークにおいては、接続される機器が比較的頻繁に変更され、かかる変更の度にアクセス許容機器リストを修正しなければならない。

【0023】

【特許文献1】

特開 2002-73861号公報

【特許文献2】

特開平 10-271154号公報

【0024】

【発明が解決しようとする課題】

本発明の目的は、ルータ経由で外部ネットワークに接続されているホーム・ネットワーク上において機器間でのコンテンツの利用を好適に管理することができる

る、優れた機器間認証システム及び機器間認証方法、通信装置、並びにコンピュータ・プログラムを提供することにある。

【0025】

本発明のさらなる目的は、ホーム・ネットワーク上の各クライアント端末がホーム・サーバ上で正当に取得されているコンテンツを著作権法で認められる私的使用の範囲内で利用するように好適に管理することができる、優れた機器間認証システム及び機器間認証方法、通信装置、並びにコンピュータ・プログラムを提供することにある。

【0026】

【課題を解決するための手段及び作用】

本発明は、上記課題を参酌してなされたものであり、その第1の側面は、ルータ経由で外部ネットワークに接続可能なホーム・ネットワーク上の機器を認証する機器間認証システムであって、前記ホーム・ネットワーク上の機器に対してアクセスする他の機器が前記ホーム・ネットワーク上に存在するかどうかを確認するローカル環境管理手段を備えることを特徴とする機器間認証システムである。

【0027】

但し、ここで言う「システム」とは、複数の装置（又は特定の機能を実現する機能モジュール）が論理的に集合した物のことを言い、各装置や機能モジュールが単一の筐体内にあるか否かは特に問わない。

【0028】

ここで、一方の機器は、ホーム・サーバであり、前記ルータ経由で外部ネットワークから、あるいはパッケージ・メディアや放送受信などを介して、コンテンツを正当に取得する。また、他方の機器はホーム・サーバに対してコンテンツを要求し利用するクライアントである。そして、双方の機器が同じホーム・ネットワーク上に存在することが確認されたことに応じて、前記ホーム・サーバは前記クライアントに対しコンテンツの提供及び／又はコンテンツに関するライセンスの発行を行なう。

【0029】

著作権法の下、著作物としてのコンテンツは無断の複製や改竄などの不正使用

から保護を受ける。一方、著作物の正当な利用者においては、私的な使用、すなわち個人的に又は家庭内その他これに順ずる限られた範囲内において使用することを目的としてコンテンツを複製することが許されている。

【0030】

そこで、本発明では、ホーム・ネットワーク内のクライアント端末は、私的な使用の範囲内にあるという前提に立ち、ローカル環境下のクライアントに限り、ホーム・サーバ上に蓄積されているコンテンツを利用することができるようにした。

【0031】

前記ホーム・ネットワーク上には2台以上のホーム・サーバを設置可能である。このような場合、各ホーム・サーバは、同じホーム・ネットワーク上のクライアント端末はローカル環境下にあることから、それぞれ独自にこれらをメンバー登録してグループを形成し、コンテンツ配信並びにコンテンツ使用のライセンスを発行する。さらに、クライアント端末は、同じホーム・ネットワーク上の2台以上のホーム・サーバに対し同時にメンバー登録し複数のグループに所属し、各々のホーム・サーバからコンテンツのライセンスを取得することができる。

【0032】

この場合も、クライアント端末は、それぞれのホーム・サーバにとってローカル環境下に存在し、個人的又は家庭の範囲内での使用であると推定されるから、ローカル環境内の各ホーム・サーバのコンテンツを自由に使用することが相当である。

【0033】

一方、クライアント端末が複数のホーム・サーバに同時にメンバー登録できるからといって、時間差をおいて、複数のホーム・ネットワークに跨って複数のホーム・サーバのグループに所属することまでは認めるべきでない。別のホーム・ネットワークに接続した時点で、元の接続先のホーム・ネットワークから見ればクライアント端末がリモート環境に移動したことに相当し、あるいは、あるホーム・ネットワークに接続した時点で他のホーム・ネットワークにとってクライアント端末はリモート環境に存在することに等しいからである。

【0034】

したがって、クライアントは、同じホーム・ネットワーク上の複数のホーム・サーバから取得したコンテンツを利用可能であるが、別のホーム・ネットワーク上のホーム・サーバに接続した時点で、それ以外のホーム・ネットワーク上のホーム・サーバから取得したコンテンツを利用不能とする。

【0035】

前記ローカル環境管理手段は、例えば、アクセス要求元の機器のMACアドレスがdefault Gatewayに設定されているルータのMACアドレスに一致しないかどうかによって同じホーム・ネットワーク上に存在するかどうかを確認することができる。

【0036】

ホーム・ネットワークはホーム・ルータ経由で外部ネットワークに接続されている。そして、同じネットワークからのアクセスであれば送信元のMACアドレスが付されているが、外部からのルータ越しのアクセスの場合は送信元がルータのMACアドレスに書き換えられる。このような既存のIPプロトコルの仕組みを利用し、通信相手のMACアドレスをホーム・ルータのMACアドレスと比較することによりホーム・ネットワーク内からのアクセスであるかどうかを自動識別することができるという訳である。

【0037】

あるいは、前記ローカル環境管理手段は、各機器がホーム・ネットワークに関する同じ識別情報を共有するかどうかによって同じホーム・ネットワーク上に存在するかどうかを確認することができる。

【0038】

例えば、各機器はdefault Gatewayに設定されているルータのMACアドレスをホーム・ネットワークに関する識別情報として取得し、機器同士が同じdefault GatewayのMACアドレスを保持しているかどうかによって同じホーム・ネットワーク上に存在するかどうかを確認する。

【0039】

または、ホーム・ネットワーク上にネットワーク識別情報を供給するローカル

環境管理装置を設置しておき、各機器は前記ローカル環境管理装置のMACアドレスをホーム・ネットワークに関する識別情報として取得し、機器同士が同じローカル環境管理装置のMACアドレスを保持しているかどうかによって同じホーム・ネットワーク上に存在するかどうかを確認することができる。

【0040】

また、本発明の第2の側面は、ルータ経由で外部ネットワークに接続され、外部ネットワークからコンテンツを正当に取得するホーム・サーバとコンテンツを要求し利用するクライアントが存在するホーム・ネットワーク上において機器を認証するための処理をコンピュータ・システム上で実行するようにコンピュータ可読形式で記述されたコンピュータ・プログラムであって、

前記ホーム・サーバと前記クライアントが前記ホーム・ネットワーク上に存在するかどうかを確認するローカル環境管理ステップと、

双方の機器が同じホーム・ネットワーク上に存在することが前記ローカル環境管理ステップにより確認されたことに応じて、前記ホーム・サーバは前記クライアントに対しコンテンツの提供及び／又はコンテンツに関するライセンスの発行を行なうコンテンツ提供ステップと、
を具備することを特徴とするコンピュータ・プログラムである。

【0041】

本発明の第2の側面に係るコンピュータ・プログラムは、コンピュータ・システム上で所定の処理を実現するようにコンピュータ可読形式で記述されたコンピュータ・プログラムを定義したものである。換言すれば、本発明の第2の側面に係るコンピュータ・プログラムをコンピュータ・システムにインストールすることによって、コンピュータ・システム上では協働的作用が発揮され、本発明の第1の側面に係る機器間認証システムと同様の作用効果を得ることができる。

【0042】

本発明のさらに他の目的、特徴や利点は、後述する本発明の実施形態や添付する図面に基づくより詳細な説明によって明らかになるであろう。

【0043】

【発明の実施の形態】

著作権法の下、著作物としてのコンテンツは無断の複製や改竄などの不正使用から保護を受ける。一方、著作物の正当な利用者においては、私的な使用、すなわち個人的に又は家庭内その他これに順ずる限られた範囲内において使用することを目的としてコンテンツを複製することが許されている（著作権法第30条を参照のこと）。

【0044】

本発明者らは、ホーム・ネットワーク内（以下、「ローカル環境」とも呼ぶ）のクライアント端末は、私的な使用の範囲内にあるという前提に立ち、ローカル環境下のクライアントに限り、ホーム・サーバ上に蓄積されているコンテンツを利用することができるというシステムを提案する。

【0045】

ここで、ローカル環境の定義について説明しておく。

【0046】

図1には、ホーム・ネットワークの基本構成を模式的に示している。同図に示すように、家庭内に敷設されるホーム・ネットワークは、ホーム・ルータ経由でインターネットなどの外部ネットワークに接続されている。

【0047】

ホーム・ネットワーク上には、ホーム・サーバと、1以上のクライアント端末が存在する。ホーム・サーバは、ホーム・ルータ経由で外部ネットワーク上のコンテンツ・サーバから正当にコンテンツを取得し、蓄積し、家庭内でコンテンツを配信する。勿論、ホーム・サーバは、パッケージ・メディアや放送受信など、ネットワーク以外の手段により、コンテンツを取得することができる。また、各クライアント端末は、ホーム・サーバに所望のコンテンツを要求し、これを取得して利用する。

【0048】

ホーム・ネットワークに接続されているクライアント端末は、ローカル環境下に存在し、個人的又は家庭の範囲内での使用であると推定される。したがって、ホーム・サーバにおいて正当に取得されているコンテンツは、ホーム・ネットワーク上のクライアント端末は自由に使用することが相当であると思料される。そ

ここで、ホーム・サーバは、ローカル環境下のこれらクライアント端末をメンバー登録し、コンテンツ配信並びにコンテンツ使用のライセンスを発行する。勿論、クライアントの接続を無限に認めることはできないので、コンテンツを享受できる端末の台数に一定の制限を設ける必要がある。

【0049】

ローカル環境下では、クライアント端末は、ホーム・サーバからコンテンツを取得し、コピーやストリーミングなどコンテンツを利用し、さらにローカル環境外（リモート環境）にコンテンツを持ち出して利用することができる。

【0050】

一方、ホーム・ネットワーク上に存在しない、すなわちリモート環境のクライアント端末は、個人的又は家庭の範囲内での使用であるとは考えられない。リモート環境のクライアント端末にコンテンツの利用を認めると、コンテンツの利用はほぼ無制限となってしまう、コンテンツに関する著作権は保護されないに等しくなるからである。そこで、ホーム・サーバは、リモート環境のクライアントをメンバーとして登録せず、また、コンテンツのライセンスを発行しない。

【0051】

図1に示した例では、ホーム・ネットワーク上には1つのホーム・サーバしか存在しないが、勿論、2以上のホーム・サーバを同じホーム・サーバ上に設置して、各ホーム・サーバがホーム・ネットワーク内でそれぞれ独自にコンテンツの配信サービスを行なうようにしてもよい。

【0052】

図2には、2台のホーム・サーバが存在するホーム・ネットワークの構成例を示している。

【0053】

この場合、各ホーム・サーバは、同じホーム・ネットワーク上のクライアント端末はローカル環境下にあることから、それぞれ独自にこれらをメンバー登録してグループを形成し、コンテンツ配信並びにコンテンツ使用のライセンスを発行する。クライアント端末は、ホーム・サーバからコンテンツを取得し、コピーやストリーミングなどコンテンツを利用し、さらにローカル環境外（リモート環境）

にコンテンツを持ち出して利用することができる。

【0054】

さらに、クライアント端末は、同じホーム・ネットワーク上の2台以上のホーム・サーバに対し同時にメンバー登録し複数のグループに所属し、各々のホーム・サーバからコンテンツのライセンスを取得することができる。この場合も、クライアント端末は、それぞれのホーム・サーバにとってローカル環境下に存在し、個人的又は家庭の範囲内での使用であると推定されるから、ローカル環境内の各ホーム・サーバのコンテンツを自由に使用することが相当であると思料される。

【0055】

一方、クライアント端末が複数のホーム・サーバに同時にメンバー登録できるからといって、時間差をおいて、複数のホーム・ネットワークに跨って複数のホーム・サーバのグループに所属することまでは認めるべきでない（図3を参照のこと）。

【0056】

別のホーム・ネットワークに接続した時点で、元の接続先のホーム・ネットワークから見ればクライアント端末がリモート環境に移動したことに相当し、あるいは、あるホーム・ネットワークに接続した時点で他のホーム・ネットワークにとってクライアント端末はリモート環境に存在することに等しいからである。ローカル環境が個人的又は家庭の範囲内であるのに対し、リモート環境は個人的又は家庭の範囲を逸脱する。

【0057】

クライアント端末が時間差をかけて複数のホーム・ネットワークに跨って接続することは技術的には可能であるが、これに併せてコンテンツの利用を逐次許可していくと、コンテンツの利用はほぼ無制限となってしまう、コンテンツに関する著作権は保護されないに等しくなる。

【0058】

以上を総括すると、ホーム・ネットワーク上において、個人的又は家庭の範囲内での使用であると推定されるローカル環境を実現するためには、以下の事柄が

必要条件であることが導出される。

【0059】

(1) ホーム・サーバは、ホーム・ネットワーク外からのメンバー登録を認めない。

(2) 同じホーム・ネットワーク内に2台以上のホーム・サーバがあるときには、ホーム・サーバ毎にメンバー登録、グループ管理を行なう。ホーム・ネットワーク上の各クライアントは2以上のホーム・サーバに登録することができる。但し、同時登録されるホーム・サーバは同じホーム・ネットワークに存在しなければならない。

【0060】

このようなローカル環境を実現するためには、ホーム・サーバとクライアント端末間で、お互い同じホーム・ネットワーク上に存在するかどうかを識別する仕組みが必要となる。

【0061】

現状のネットワーク・プロトコルでは、ホーム・ネットワークなどネットワークをセグメント単位で識別する仕組みは提供されていない。そこで、本発明者らは、ホーム・ネットワークがホーム・ルータ経由で外部ネットワークに接続されていることを鑑み、同じネットワークからのアクセスであれば送信元のMACアドレスが付されているが、外部からのルータ越しのアクセスの場合は送信元がルータのMACアドレスに書き換えられるという既存のIPプロトコルの仕組みを利用し、通信相手のMACアドレスをホーム・ルータのMACアドレスと比較することによりホーム・ネットワーク内からのアクセスであるかどうかを自動識別する方法を提案する。

【0062】

以下、図面を参照しながら本発明の実施形態について詳解する。

【0063】

図4には、本発明の一実施形態に係るホーム・ネットワークの構成を模式的に示している。

【0064】

家庭内に敷設されるホーム・ネットワークは、ホーム・ルータ経由でインターネットなどWAN、あるいは他のLANに接続されている。ホーム・ネットワークのdefault Gatewayはホーム・ルータに設定されている。

【0065】

ホーム・ネットワークは、例えばハブ（集結装置）にホーム・サーバやクライアント端末などのホスト装置のLANケーブルを接続することにより構成される。

【0066】

ホーム・サーバやクライアント端末、ホーム・ルータなどのホーム・ネットワーク上のホスト装置、並びに外部ネットワーク上のホスト装置は、機器固有のMACアドレスを有している。ホスト装置は、受信先MACアドレス及び送信元MACアドレスを含んだヘッダ情報を持つパケット、例えばイーサネット（登録商標）フレームを、ネットワーク経由で送受信する。

【0067】

ホーム・サーバやクライアント端末などのホーム・ネットワーク上のホスト装置は、例えばUPnP対応機器として構成される。この場合、ネットワークに対する接続機器の追加や削除が容易である。ホーム・ネットワークに新たに接続する機器は、以下の手順に従って、コンテンツ利用などホーム・ネットワーク上のサービスを享受することができるようになる。

【0068】

- (1) アドレッシング処理：IPアドレスなどの自己のデバイスIDを取得する
- (2) ディスカバリ処理：ネットワーク上の各デバイスの検索を行ない、各デバイスから受信した応答に含まれるデバイス種別や機能などの情報を取得する
- (3) サービス要求処理：ディスカバリ処理で取得された情報に基づいて各デバイスにサービスを要求する

【0069】

ホーム・ネットワーク上では、個人的又は家庭の範囲内での使用であると推定されるローカル環境が形成されている。したがって、ホーム・サーバは、ホーム・ルータ経由で外部ネットワーク上のコンテンツ・サーバから正当にコンテンツ

を取得し、蓄積し、家庭内でコンテンツを配信する。また、各クライアント端末は、ホーム・サーバに所望のコンテンツを要求し、これを取得して利用することが許容される。

【0070】

ローカル環境下では、クライアント端末は、ホーム・サーバからコンテンツを取得し、コピーやストリーミングなどコンテンツを利用し、さらにローカル環境外（リモート環境）にコンテンツを持ち出して利用することができる。

【0071】

また、図5には、本発明の他の実施形態に係るホーム・ネットワークの構成を模式的に示している。

【0072】

ホーム・ネットワークは、ホーム・ルータ経由でインターネットなどWAN、あるいは他のLANに接続されている。この場合も、ホーム・ネットワークの default Gatewayはホーム・ルータに設定されている。

【0073】

図4との相違は、ホーム・ネットワーク上に2台のホーム・サーバが存在する点である。各ホーム・サーバは、ホーム・ネットワーク上に同時に存在してもよいし、あるいは時間差を以って接続されてもよい。

【0074】

この場合、各ホーム・サーバは、同じホーム・ネットワーク上のクライアント端末はローカル環境下にあることから、これらをメンバー登録してグループを形成し、コンテンツ配信並びにコンテンツ使用のライセンスを発行する。クライアント端末は、ホーム・サーバからコンテンツを取得し、コピーやストリーミングなどコンテンツを利用し、さらにローカル環境外（リモート環境）にコンテンツを持ち出して利用することができる。また、クライアント端末は、同じホーム・ネットワーク上の2台以上のホーム・サーバに対し同時にメンバー登録し複数のグループに所属し、各々のホーム・サーバからコンテンツのライセンスを取得することができる。

【0075】

図6には、サーバやクライアントなどとしてホーム・ネットワークに接続されるホスト装置のハードウェア構成を模式的に示している。

【0076】

このシステムは、プロセッサ10を中心に構成されている。プロセッサ10は、メモリに記憶されたプログラムに基づいて各種の処理を実行する。また、プロセッサは、バス30を介して接続されている各種の周辺機器を制御している。バス30に接続された周辺機器は次のようなものである。

【0077】

メモリ20は、例えばDRAM (Dynamic RAM) などの半導体メモリで構成され、プロセッサ10において実行されるプログラム・コードをロードしたり、実行プログラムの作業データを一時格納したりするために使用される。

【0078】

ディスプレイ・コントローラ21は、プロセッサ10から送られてくる描画命令に従って表示画像を生成し、表示装置22に送る。ディスプレイ・コントローラに接続された表示装置22は、ディスプレイ・コントローラ21から送られた表示画像情報に従い、その画像を画面に表示出力する。

【0079】

入出力インターフェース23は、キーボード24やマウス25が接続されており、キーボード24やマウス25からの入力信号をプロセッサ10へ転送する。

【0080】

ネットワーク・インターフェース26は、LANやインターネットなどの外部ネットワークに接続されており、インターネットを介したデータ通信を制御する。すなわち、プロセッサ10から送られたデータをインターネット上の他の装置へ転送するとともに、インターネットを介して送られてきたデータを受け取りプロセッサ10に渡す。

【0081】

ハード・ディスク装置 (HDD: Hard Disk Drive) コントローラ27には、HDDなどの大容量外部記憶装置28が接続されており、HDDコントローラ27が接続されたHDD28へのデータの入出力を制御する。HD

D28には、プロセッサが実行すべきオペレーティング・システム（OS）のプログラム、アプリケーション・プログラム、ドライバ・プログラムなどが格納されている。アプリケーション・プログラムは、例えば、ホーム・サーバとしてホーム・ネットワーク上の各クライアント端末の認証処理を行ったり、コンテンツの提供やライセンスの発行を行ったりするサーバ・アプリケーションや、サーバから提供されたコンテンツの再生などコンテンツの利用を行なうクライアント・アプリケーションなどである。

【0082】

なお、ホスト装置を構成するためには、図6に示した以外にも多くの電気回路などが必要である。但し、これらは当業者には周知であり、また、本発明の要旨を構成するものではないので、本明細書中では省略している。また、図面の錯綜を回避するため、図中の各ハードウェア・ブロック間の接続も一部しか図示していない点を了承されたい。

【0083】

図7には、本実施形態に係るホーム・ネットワーク上での動作を示している。但し、ネットワーク上にはクライアント端末と、2台のホーム・サーバと、ホーム・ルータが少なくとも存在し、ホーム・ルータがdefault Gatewayに設定されているものとする。

【0084】

クライアント端末は、ホーム・サーバからコンテンツを取得し、コピーやストリーミングなどコンテンツを利用するが、各ホーム・サーバはコンテンツ配信サービスの開始に先立ち、ホーム・ルータからdefault GatewayのMACアドレスを取得しておく。

【0085】

クライアント端末は、サーバにアクセスする際、まずホーム・ルータからdefault GatewayのMACアドレスを取得し、取得したMACアドレスを付してサーバにアクセス要求を送信する。

【0086】

アクセス要求されたサーバ側では、要求パケットから送信元のMACアドレス

を取り出して、これを自身があらかじめ取得しておいた `default Gateway` のMACアドレスと比較する。同じネットワークからのアクセスであれば送信元のMACアドレスが付されているが、外部からのルータ越しのアクセスの場合は送信元がルータのMACアドレスに書き換えられる。したがって、送信元のMACアドレスが `default Gateway` のMACアドレスと一致するかどうかによって、要求元のクライアントが同じホーム・ネットワークすなわちローカル環境に置かれているかどうかを簡易に判別することができる。そして、ローカル環境に置かれている場合には要求されたコンテンツを配信するとともにそのライセンスを発行するが、ローカル環境に置かれていない場合は要求を拒否する。このようにして形成されたローカル環境内においてのみ、機器間でコンテンツの利用を認めることにより、コンテンツの不正流通を効果的に抑制することができる。

【0087】

クライアント端末は、要求先サーバから返送パケットを受け取ると、サーバのMACアドレスとサーバ名を取り出し、これをアクセス要求に先立って取得した `default Gateway` のMACアドレスと組にしてローカル環境管理テーブルに格納しておく。

【0088】

図8には、ローカル環境管理テーブルの構成を模式的に示している。図示のローカル環境管理テーブルは、新たなサーバに対してコンテンツ要求が行なわれる度にレコードがエントリされる。各レコードはLASTフラグと、ネットワーク識別IDと、サーバのMACアドレスと、サーバ名が格納される。ネットワーク識別IDには、サーバ・アクセス時に先立って取得された `default Gateway` のMACアドレスが記載される。また、LASTフラグは、最後にアクセスされたサーバのレコードにフラグが設定されるようになっている。

【0089】

図8に示す例では、クライアント端末は、ホーム・ルータAに接続されているホーム・ネットワーク上のサーバS1、ホーム・ルータAに接続されているホーム・ネットワーク上のサーバS2、並びにホーム・ルータBに接続されているホ

ーム・ネットワーク上のサーバS3にアクセスした履歴が示されている。また、クライアント端末が最後にアクセスしたのはホーム・ルータAに接続されているホーム・ネットワーク上のサーバS2である。

【0090】

クライアント端末は、同じホーム・ネットワーク上の2台以上のホーム・サーバに対し同時にメンバー登録し複数のグループに所属し、各々のホーム・サーバからコンテンツのライセンスを取得することができる。この場合、クライアント端末は、それぞれのホーム・サーバにとってローカル環境下に存在し、個人的又は家庭の範囲内での使用であると推定されるからである。

【0091】

他方、クライアント端末が時間差をかけて別のホーム・ネットワークに接続した場合、その時点で、元の接続先のホーム・ネットワークから見ればクライアント端末がリモート環境に移動したことに相当する。クライアント端末がサーバにアクセスする際に所得するdefault GatewayのMACアドレスをローカル環境管理テーブル上で照合し、ホーム・ネットワーク間で移動したかどうかを判別することができる。

【0092】

クライアント端末は、ホーム・サーバからコンテンツを取得し、コピーやストリーミングなどコンテンツを利用し、さらにローカル環境外（リモート環境）にコンテンツを持ち出して利用することができる。但し、時間差をかけて複数のホーム・ネットワークに接続して、逐次取得されるコンテンツを無制限に利用することは認められない。そこで、本実施形態では、クライアント端末上でのコンテンツの利用は、現在接続しているホーム・ネットワークから取得されたものに制限するようにしている。

【0093】

図8に示したローカル環境管理テーブル中のLASTフラグは、最後にアクセスされたホーム・サーバを指示する。本実施形態では、最後にアクセスしたホーム・サーバが存在するホーム・ネットワークがクライアント端末の現在のローカル環境であると規定する。したがって、LASTフラグが付されたホーム・サー

バと同じ default Gateway の MAC アドレスを持つホーム・サーバはローカル環境に存在すると推定される。

【0094】

図9には、クライアント端末上でコンテンツを利用するときの処理手順をフローチャートの形式で示している。クライアント端末上でコンテンツを利用（再生）しようとするとき、ローカル環境管理テーブルを参照し、LASTフラグが設定されているレコードと同じ default Gateway の MAC アドレスを持つサーバが他にあるかどうかを判別し（ステップS1）、同じ MAC アドレスを持つサーバから取得したコンテンツを利用可能にし（ステップS2）、それ以外のサーバから取得したコンテンツを利用不能にする（ステップS3）。

【0095】

上述した実施形態では、同じネットワークからのアクセスであれば送信元の MAC アドレスが付されているが、外部からのルータ越しのアクセスの場合は送信元がルータの MAC アドレスに書き換えられるという既存の IP プロトコルの仕組みを利用し、通信相手の MAC アドレスをホーム・ルータの MAC アドレスと比較することによりホーム・ネットワーク内からのアクセスであるかどうかを自動識別するというものであった。但し、ホスト装置が同じホーム・ネットワーク上にあることを識別する方法はこれに限定されない。

【0096】

図10には、図4に示したホーム・ネットワークの変形例を示している。

【0097】

図示の例では、ホーム・ネットワークは、ホーム・ルータ経由でインターネットなど WAN、あるいは他の LAN に接続されている。ホーム・ネットワークの default Gateway はホーム・ルータに設定されるが、これは任意である。

【0098】

ホーム・ネットワークは、ハブにホーム・サーバやクライアント端末などのホスト装置の LAN ケーブルを接続することにより構成される。本実施形態では、ホーム・ネットワークに対して識別機能を付与するローカル識別装置がホーム・

ネットワークに接続されている点が図4とは相違する。

【0099】

ホーム・ネットワーク上では個人的又は家庭の範囲内での使用であると推定されるローカル環境が形成されている。したがって、ホーム・サーバは、ホーム・ルータ経由で外部ネットワーク上のコンテンツ・サーバから正当にコンテンツを取得し、蓄積し、家庭内でコンテンツを配信する。また、各クライアント端末は、ホーム・サーバに所望のコンテンツを要求し、これを取得して利用することが許容される（同上）。

【0100】

図11には、図10に示したホーム・ネットワーク上での動作を示している。

【0101】

クライアント端末は、ホーム・サーバからコンテンツを取得し、コピーやストリーミングなどコンテンツを利用するが、各ホーム・サーバはコンテンツ配信サービスの開始に先立ち、ローカル識別装置のMACアドレスを取得しておく。

【0102】

クライアント端末は、サーバにアクセスする際、まずローカル識別装置のMACアドレスを取得し、取得したMACアドレスを付してホーム・サーバにアクセス要求を送信する。

【0103】

アクセス要求されたサーバ側では、要求パケットからローカル識別装置のMACアドレスを取り出して、これを自身があらかじめ取得しておいたローカル識別装置のMACアドレスと比較する。そして、両者のMACアドレスと一致するかどうかによって、要求元のクライアントが同じホーム・ネットワークすなわちローカル環境に置かれているかどうかを簡易に判別する。ローカル環境に置かれている場合には要求されたコンテンツを配信するとともにそのライセンスを発行するが、ローカル環境に置かれていない場合は要求を拒否する。このようにして形成されたローカル環境内においてのみ、機器間でコンテンツの利用を認めることにより、コンテンツの不正流通を効果的に抑制することができる。

【0104】

クライアント端末は、要求先サーバから返送パケットを受け取ると、サーバの MAC アドレスとサーバ名を取り出し、これをアクセス要求に先立って取得したローカル識別装置の MAC アドレスと組にしてローカル環境管理テーブルに格納しておく。この場合のローカル環境管理テーブルの各レコードには、ネットワーク識別 ID には、default Gateway の MAC アドレスに代えて、ローカル識別装置の MAC アドレスが記載される。

【0105】

図 12 には、図 10 に示したホーム・ネットワークの変形例を示している。図示の通り、ローカル識別装置は、専用機としてホーム・ネットワークに接続される以外に、ホーム・ルータあるいはホーム・ネットワーク上の他のホスト装置に組み込んで構成することができる。

【0106】

ローカル識別装置の必要条件として、クライアント端末からの要求に常時応答できることを挙げることができる。このため、ローカル識別装置は常に電源が投入された状態であり、且つ、家庭内に最低 1 台あることが好ましい。ホーム・サーバは、例えば TV 受像機やビデオ録画再生装置などであり、これらの機器は常時起動しているとは限らないので（電源が投入されていないためにローカル環境を確認できなくなる）、ローカル識別装置の要件として不十分である。一方、冷蔵庫は、一家に一台あり、常に電源が投入されていることから、ローカル識別装置としての要件を満たしている。加えて、冷蔵庫は重量物で、固定的・移動不能であることから、外部に持ち出して不正を働くことが困難であるという副次的な効果もある。

【0107】

なお、ローカル識別装置は、1 つのホーム・ネットワーク上に 2 台以上存在していてもよい。この場合、クライアント端末がローカル識別装置を指定して認証を要求し、あるいは逆にサーバがローカル識別装置を指定して認証を要求する。または、クライアント端末がローカル識別装置にサーバを指定して認証を要求し、ローカル識別装置がサーバと認証を行なう。

【0108】

本明細書で説明した実施形態では、機器間の認証に機器のMACアドレスの照合を用いているが、ホーム・ルータやローカル識別装置はMACアドレスを暗号的な手段を用いて偽装困難な形で保持していることを前提とする。

【0109】

[追補]

以上、特定の実施形態を参照しながら、本発明について詳解してきた。しかしながら、本発明の要旨を逸脱しない範囲で当業者が該実施形態の修正や代用を成し得ることは自明である。すなわち、例示という形態で本発明を開示してきたのであり、本明細書の記載内容を限定的に解釈すべきではない。本発明の要旨を判断するためには、冒頭に記載した特許請求の範囲の欄を参酌すべきである。

【0110】

【発明の効果】

以上詳記したように、本発明によれば、ルータ経由で外部ネットワークに接続されているホーム・ネットワーク上で機器間でのコンテンツの利用を好適に管理することができる、優れた機器間認証システム及び機器間認証方法、通信装置、並びにコンピュータ・プログラムを提供することができる。

【0111】

また、本発明によれば、ホーム・ネットワーク上の各クライアント端末がホーム・サーバ上で正当に取得されているコンテンツを著作権法で認められる私的使用の範囲内で利用するように好適に管理することができる、優れた機器間認証システム及び機器間認証方法、通信装置、並びにコンピュータ・プログラムを提供することができる。

【0112】

本発明によれば、ローカル環境内においてのみ、機器間でコンテンツの利用を認めることにより、コンテンツの不正流通を効果的に抑制することができる。

【図面の簡単な説明】

【図1】

ホーム・ネットワークの基本構成を模式的に示した図である。

【図2】

2 台のホーム・サーバが存在するホーム・ネットワークの構成例を示した図である。

【図 3】

クライアント端末が複数のホーム・ネットワークに跨って接続する様子を示した図である。

【図 4】

本発明の一実施形態に係るホーム・ネットワークの構成を模式的に示した図である。

【図 5】

本発明の他の実施形態に係るホーム・ネットワークの構成を模式的に示した図である。

【図 6】

サーバやクライアントなどとしてホーム・ネットワークに接続されるホスト装置のハードウェア構成を模式的に示した図である。

【図 7】

本発明に係るホーム・ネットワーク上での動作シーケンスを示した図である。

【図 8】

ローカル環境管理テーブルの構成を示した図である。

【図 9】

クライアント端末上でコンテンツを利用するときの処理手順を示したフローチャートである。

【図 10】

図 4 に示したホーム・ネットワークの変形例を示した図である。

【図 11】

本発明に係るホーム・ネットワーク上での動作シーケンスを示した図である。

【図 12】

図 10 の変形例を示した図である。

【符号の説明】

10…プロセッサ

20…メモリ

21…ディスプレイ・コントローラ

22…表示装置

23…入出力インターフェース

24…キーボード

25…マウス

26…ネットワーク・インターフェース

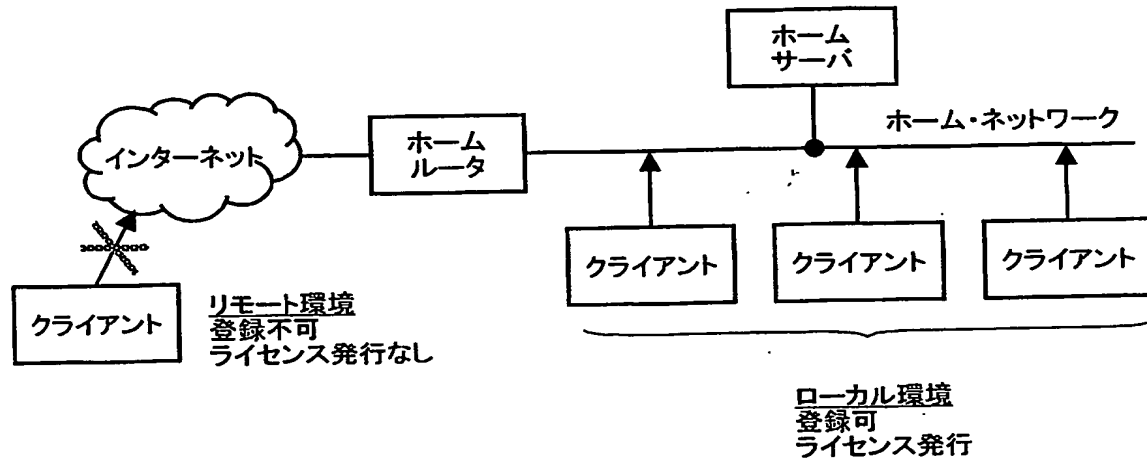
27…ハード・ディスク装置コントローラ

28…HDD

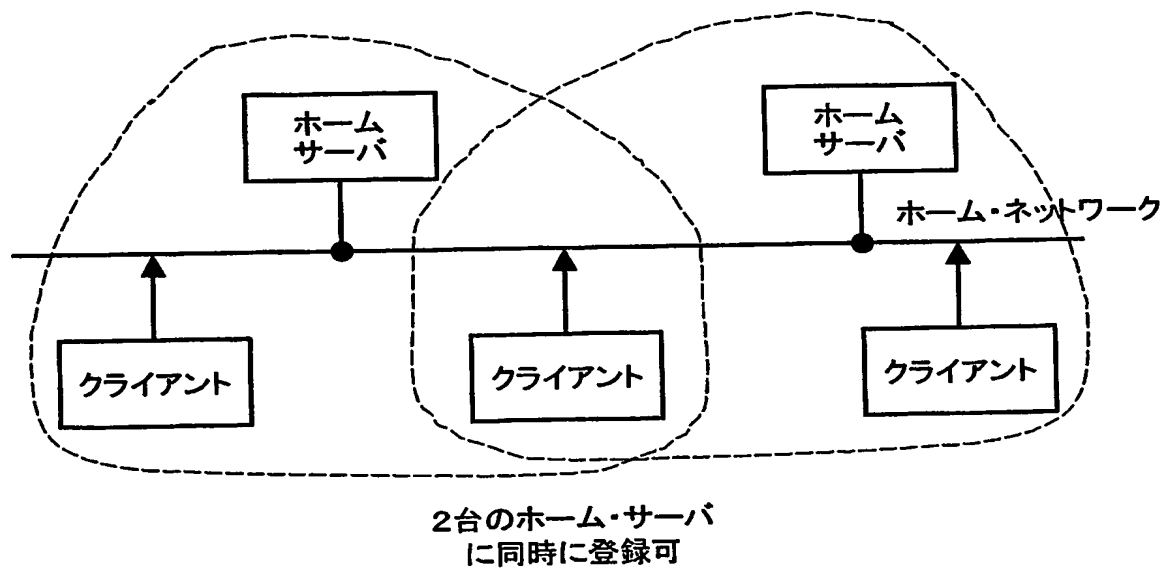
30…バス

【書類名】 図面

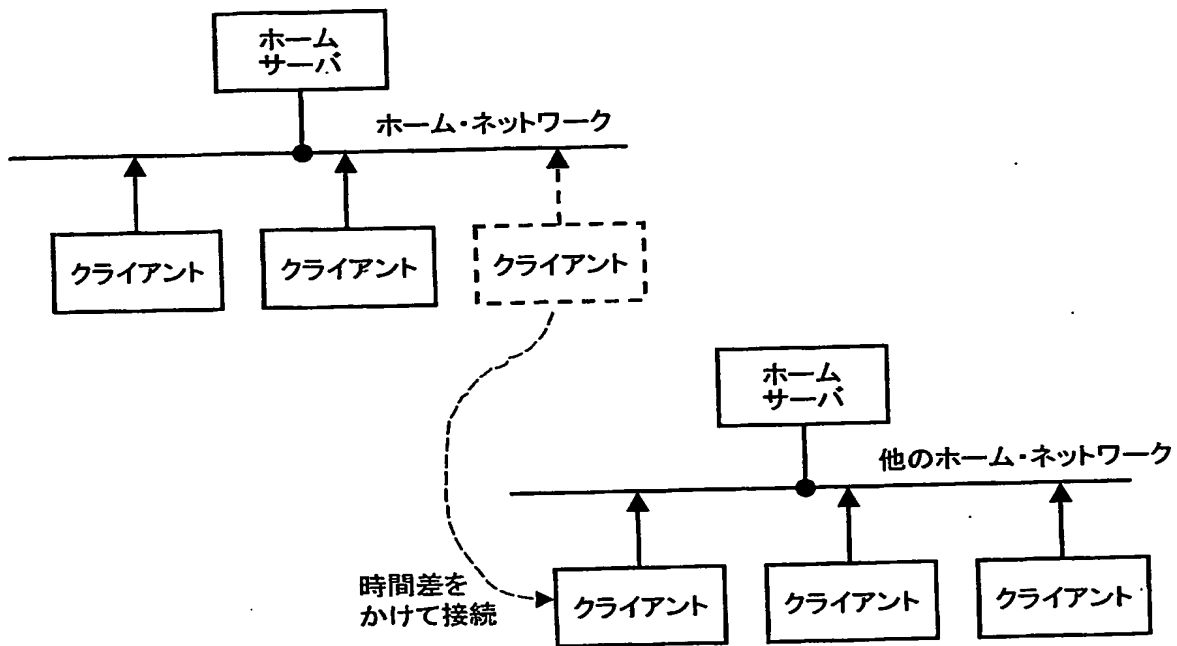
【図 1】



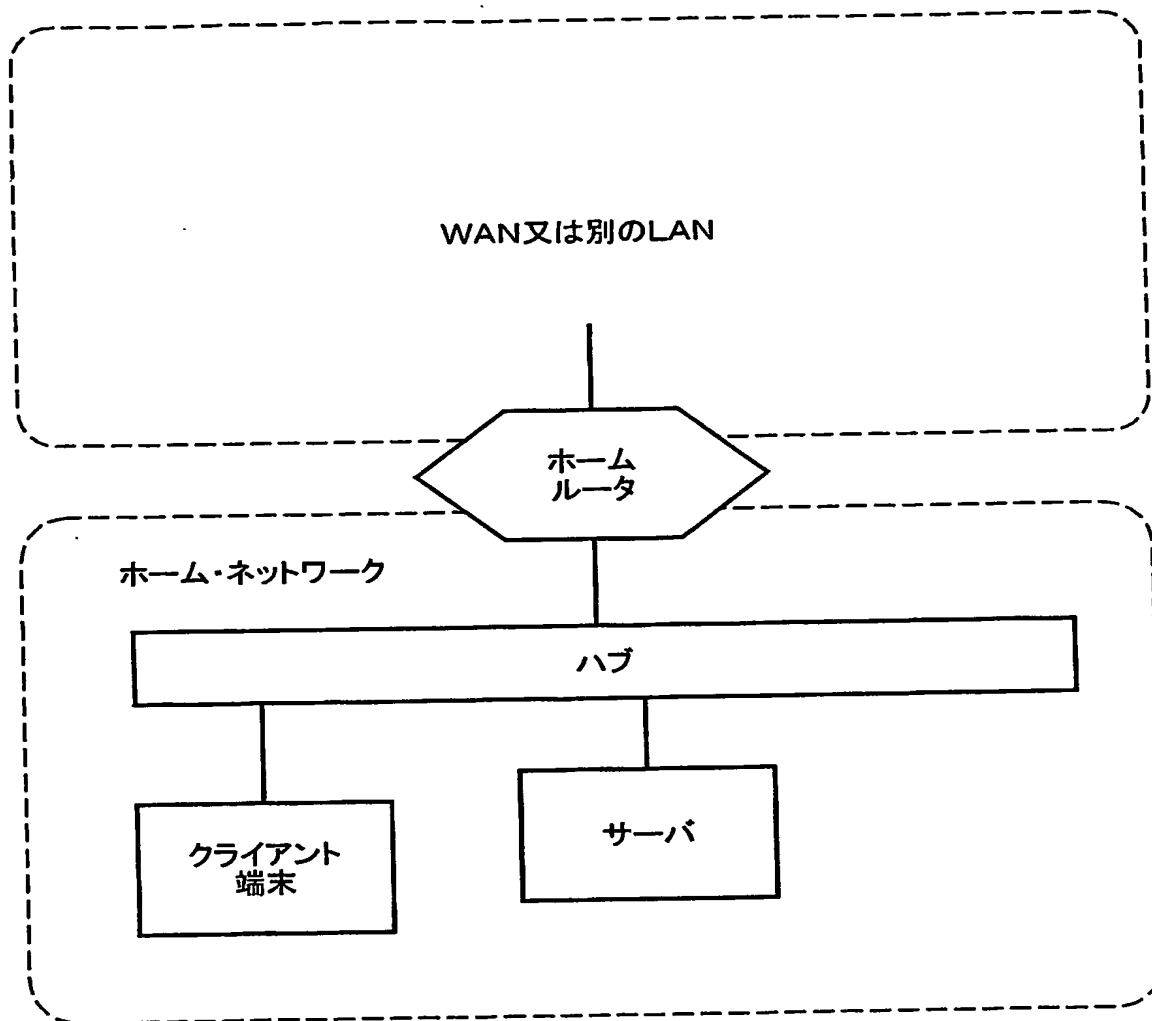
【図 2】



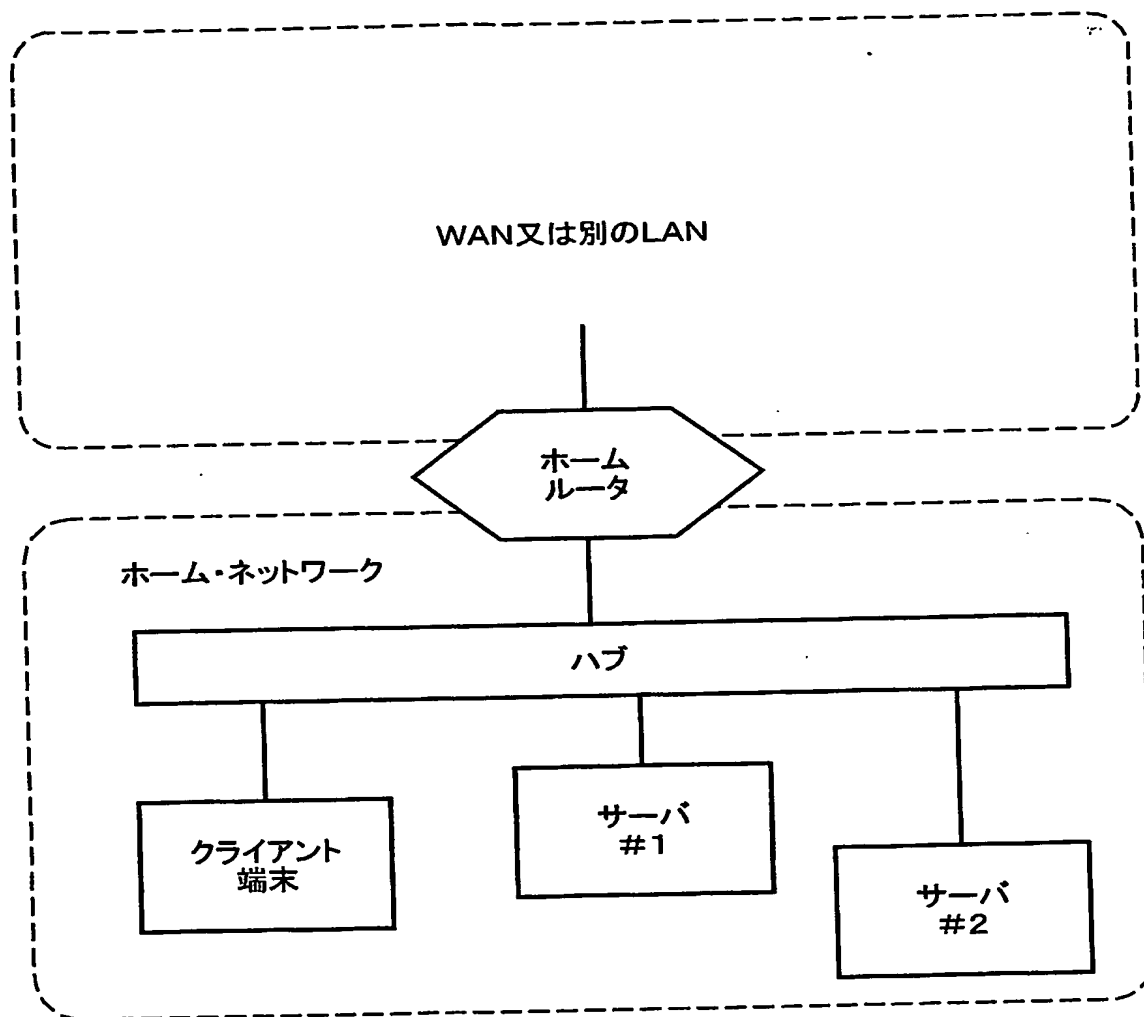
【図3】



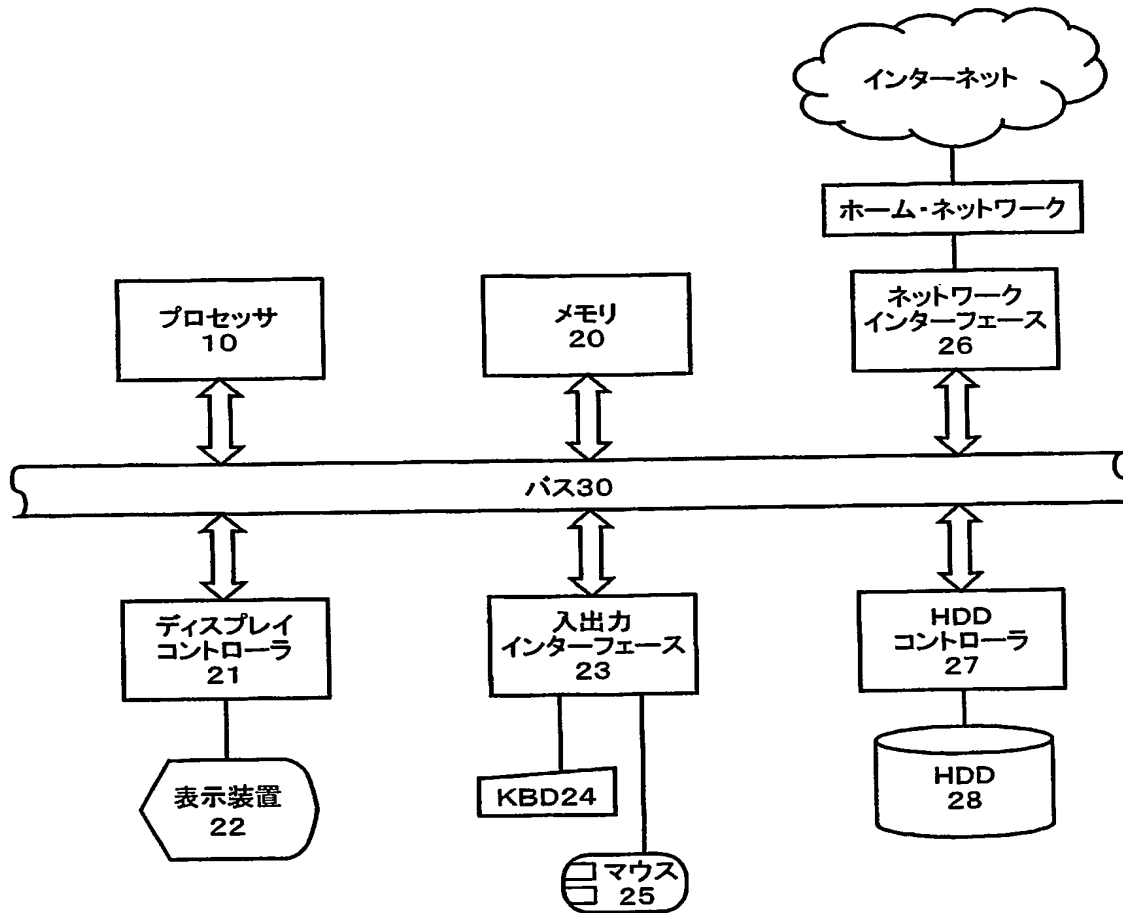
【図4】



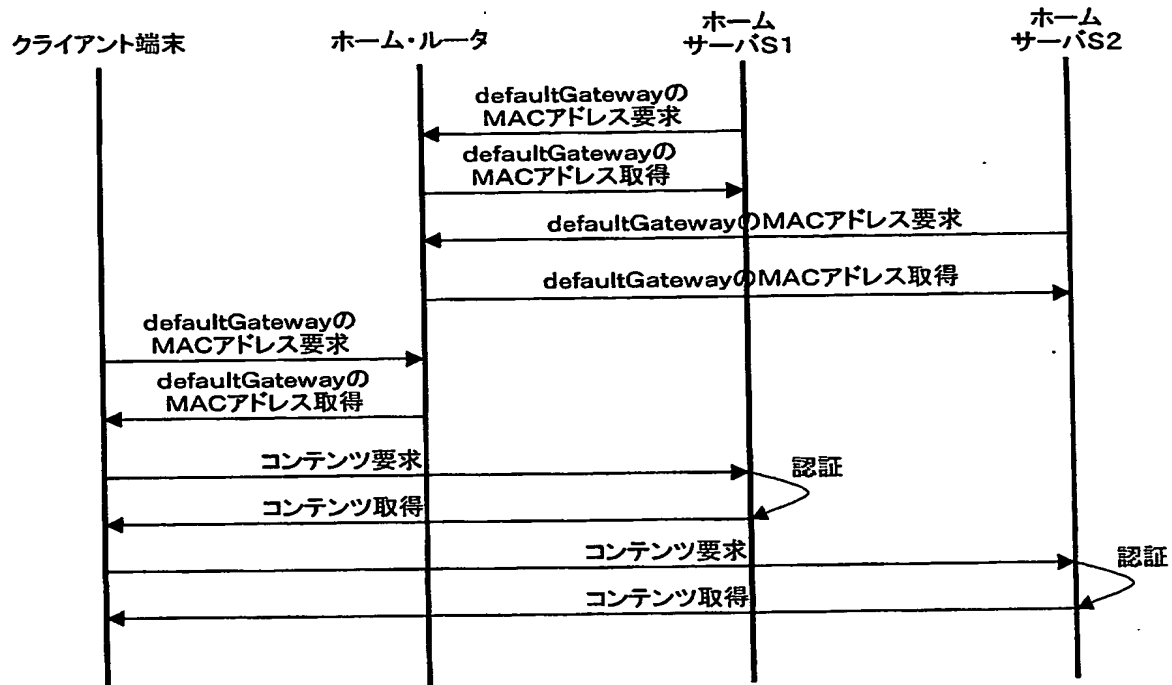
【図5】



【図6】



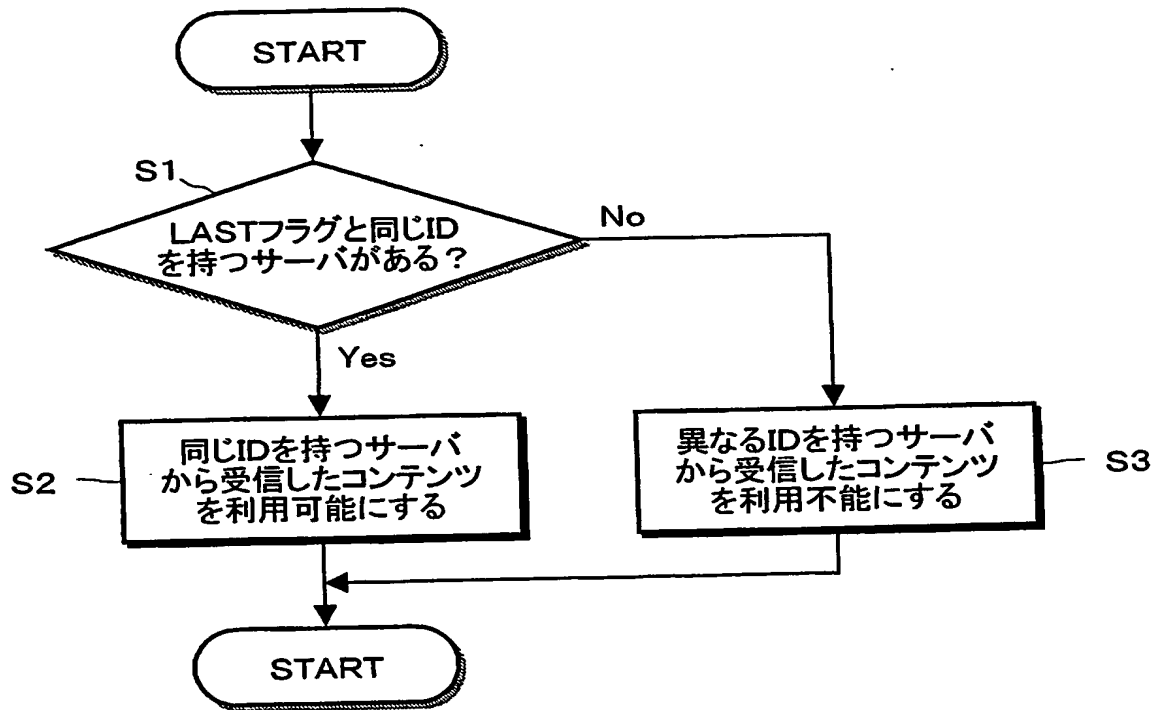
【図 7】



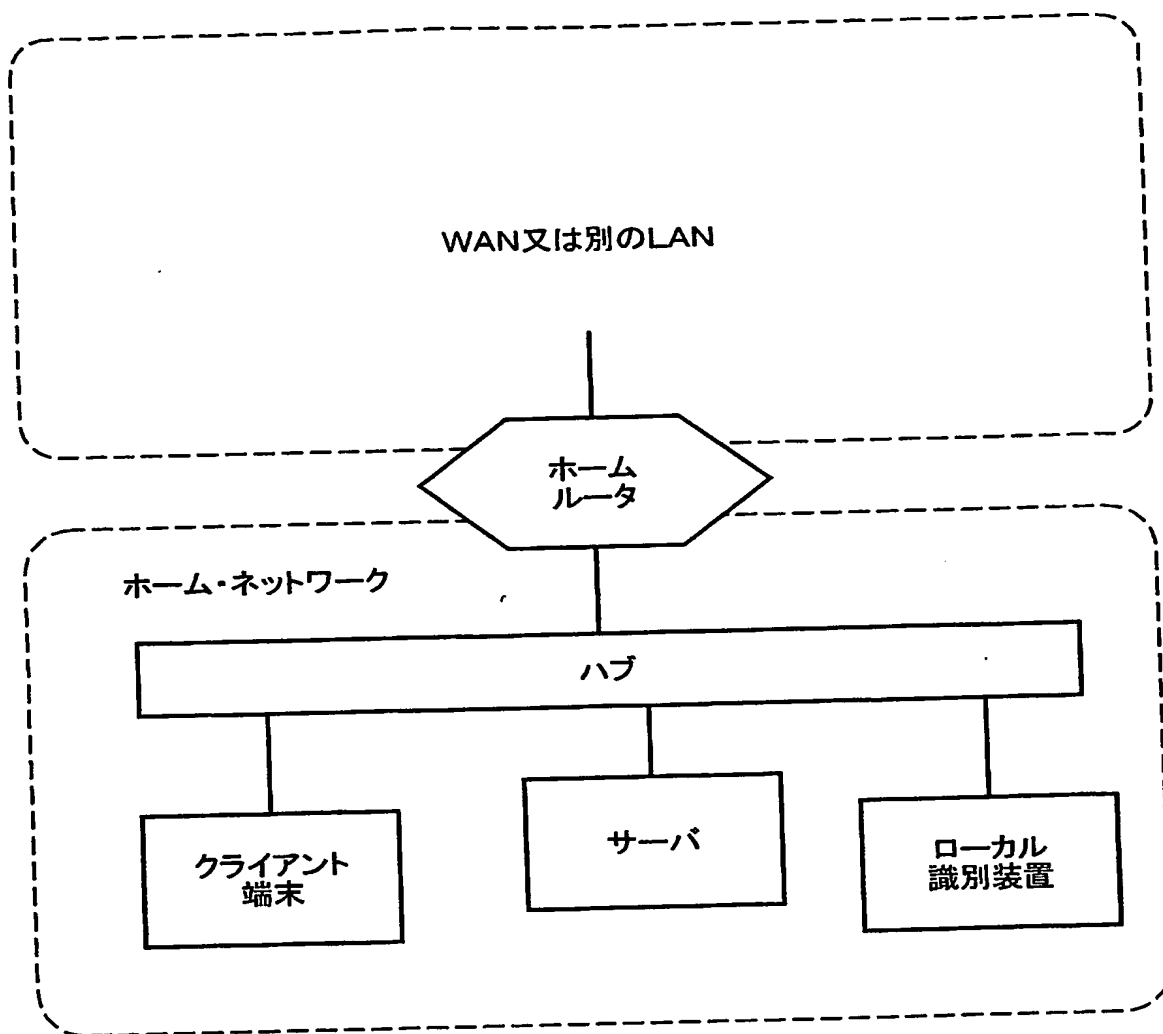
【図 8】

LAST フラグ	ネットワーク識別ID	サーバのMACアドレス	サーバ名
	ホーム・ルータAの defaultGateway	サーバS1のMACアドレス	サーバS1
✓	ホーム・ルータAの defaultGateway	サーバS2のMACアドレス	サーバS2
	ホーム・ルータBの defaultGateway	サーバS3のMACアドレス	サーバS3

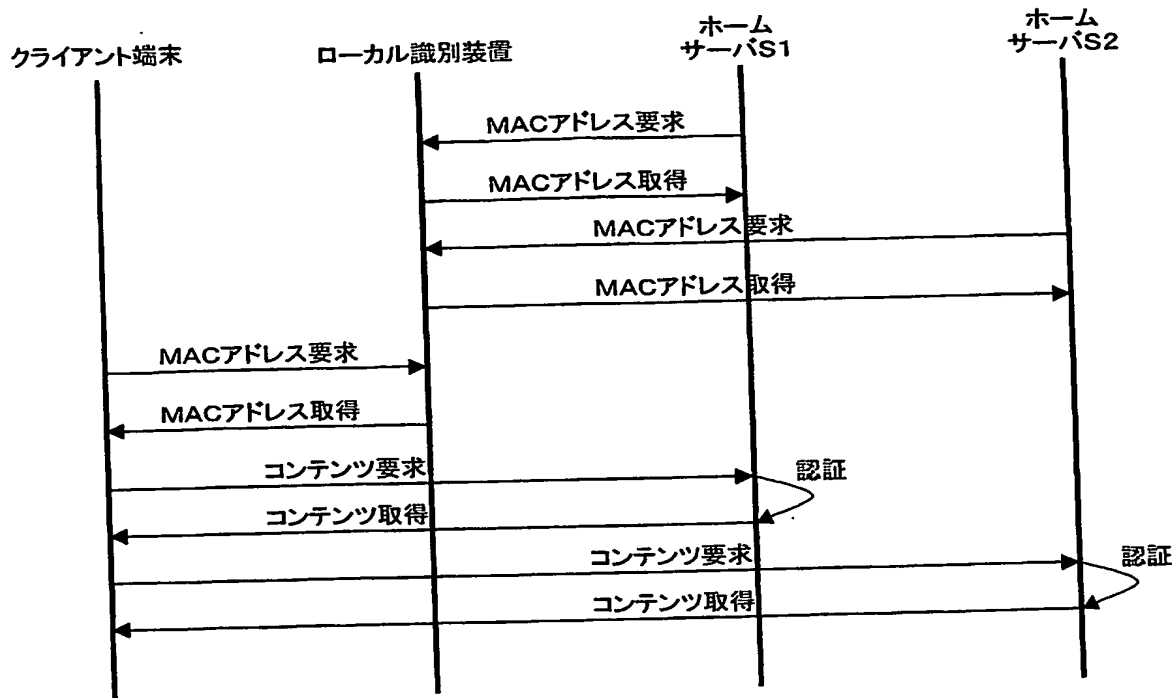
【図9】



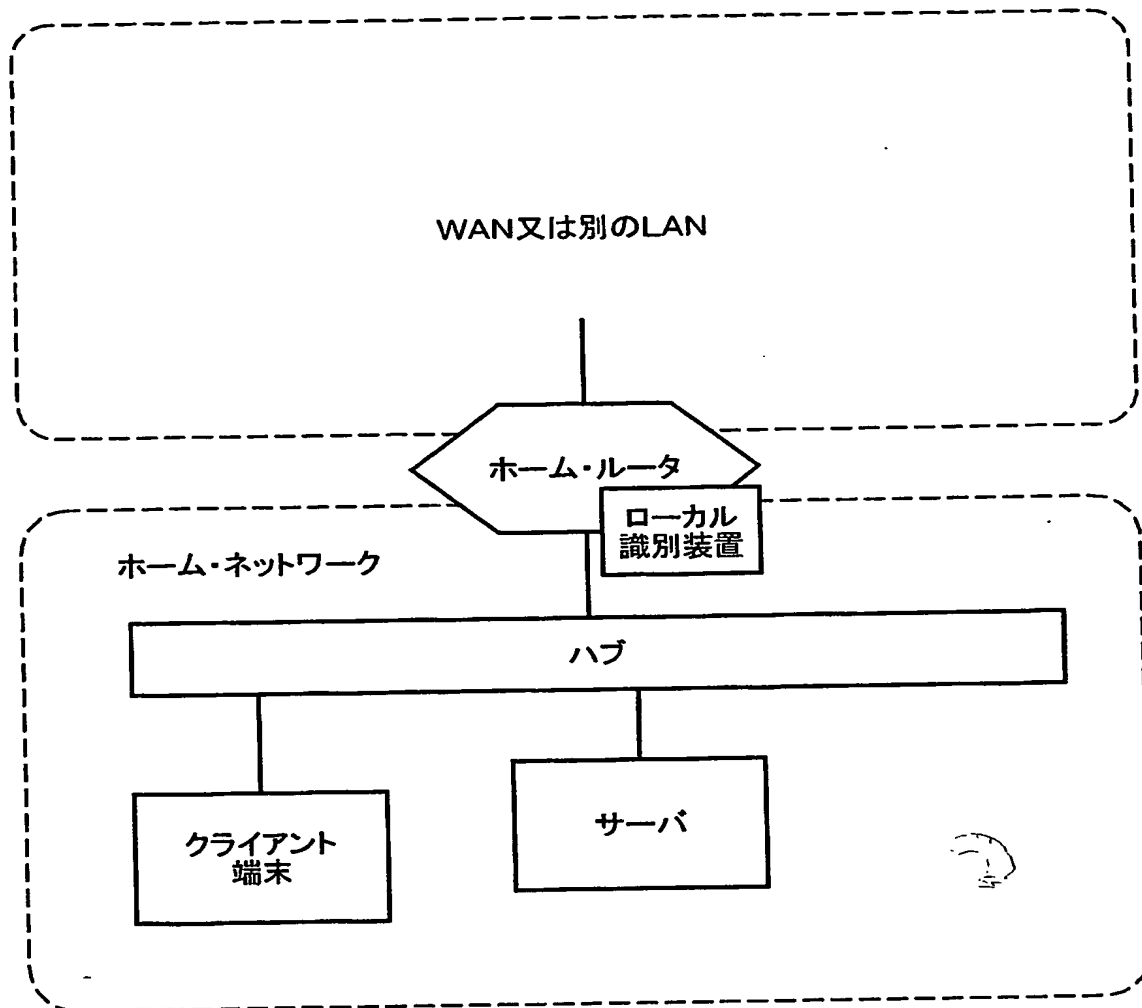
【図10】



【図11】



【図12】



【書類名】 要約書

【要約】

【課題】 ホーム・サーバ上で正当に取得されているコンテンツを著作権法で認められる私的使用の範囲内でクライアント端末が利用するように管理する。

【解決手段】 ホーム・ネットワークがホーム・ルータ経由で外部ネットワークに接続されていることを鑑み、同じネットワークからのアクセスであれば送信元のMACアドレスが付されているが、外部からのルータ越しのアクセスの場合は送信元がルータのMACアドレスに書き換えられることを利用し、通信相手のMACアドレスをホーム・ルータのMACアドレスと比較することによりホーム・ネットワーク内からのアクセスであるかどうかを自動識別する。

【選択図】 図1

特願 2003-132903

出 願 人 履 歴 情 報

識別番号

[000002185]

1. 変更年月日

1990年 8月30日

[変更理由]

新規登録

住 所

東京都品川区北品川6丁目7番35号

氏 名

ソニー株式会社